Remarks

The Office Action mailed March 23, 2005 has been carefully reviewed and the following remarks have been made in consequence thereof.

Claims 16-22, 24-25, and 27-31 are now pending in this application. Claims 16-20 and 23-31 are rejected. Claims 21 and 22 are objected to. Claims 1-15, 23, and 26 are canceled without prejudice, waiver, or disclaimer. Claims 16-18, 20, 24, 25, and 27-31 have been amended. No new matter has been added.

Applicants acknowledge that the restriction requirement has been made final, and Applicants have cancelled Claims 1-15, which were withdrawn from prosecution as a result of the restriction requirement.

The rejection of Claims 16-19 and 23-31 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow (U.S. Patent No. 6,061,668) in view of Elgamal et al. (U.S. Patent 5,825,890) is respectfully traversed.

Sharrow describes a central management computer (10) that uses a data format to transmit instructions, acknowledgments, and messages to appliances and machines on a network (column 3, lines 12-16). The central management computer checks for an acknowledgment for each transmission sent, and sends an acknowledgment for every data transmission correctly received (column 3, lines 23-26).

Elgamal et al. describe a SEQUENCE-NUMBER, which is a counter incremented by both a sender and a receiver (column 18, lines 24-25). For each transmission direction, a pair of counters is kept, one by the sender, and one by the receiver (column 18, lines 25-27). Every time a message is sent by the sender the counter is incremented (column 18, lines 27-28).

Claim 16 recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication center and the first appliance; maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter; generating a first authentication word by applying an appliance message and the first shared message counter, as stored in the communication center, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the first appliance."

Neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 16. Specifically, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter. Rather, Sharrow describes checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe incrementing a counter incremented by a sender and a receiver. Elgamal et al. further describe employing a pair of counters by the sender and the receiver for each transmission direction. Accordingly, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and an appliance and that provides a count separate from a count provided by the first shared message counter. For the

reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Elgamal et al.

Claim 23 has been canceled. Claims 17-19 and 24 depend, directly or indirectly, from independent Claim 16. When the recitations of Claims 17-19 and 24 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claims 17-19 and 24 likewise are patentable over Sharrow in view of Elgamal et al.

Claim 25 recites a system comprising "a plurality of appliances including a first appliance and a second appliance; and an appliance communication center including: network connections terminating at the appliances; a processing circuit; a memory storing a plurality of shared counters including a first shared message counter and a second shared message counter, the first shared message counter shared between the appliance communication center and the first appliance, the second shared message counter shared between the communication center and the second appliance, the first shared message counter configured to provide a count separate from a count provided by the second shared message counter, the first and second shared message counters configured to be non-resettable, the memory further storing instructions for: maintaining at an appliance communication center the first shared message counter; generating a first authentication word by applying an appliance message and the first shared message counter, as stored in the appliance communication center, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the first appliance."

Neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest a system as recited in Claim 25. Specifically, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest a memory storing a plurality of shared counters including a first shared message counter and a second shared message counter, the first shared message counter shared between the appliance communication center and the first appliance, the second shared message counter shared between the communication center and the second appliance, the first shared message counter configured

to provide a count separate from a count provided by the second shared message counter, the first and second shared message counters configured to be non-resettable. Rather, Sharrow describes checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe incrementing a counter incremented by a sender and a receiver. Elgamal et al. further describe employing a pair of counters by the sender and the receiver for each transmission direction. Accordingly, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest a memory storing a plurality of shared counters including a first shared message counter and a second shared message counter shared between the appliance communication center and the second appliance, where the first shared message counter provides a count separate from a count provided by the second shared message counter, and the first and second shared message counters are non-resettable. For the reasons set forth above, Claim 25 is submitted to be patentable over Sharrow in view of Elgamal et al.

Claim 26 has been canceled. Claim 27 depends from independent Claim 25. When the recitations of Claim 27 are considered in combination with the recitations of Claim 25, Applicants submit that dependent Claim 27 likewise is patentable over Sharrow in view of Elgamal et al.

Claim 28 recites a system comprising "a first appliance including: a first shared message counter; a processor; and a memory coupled to the processor, the memory storing instructions for execution by the processor for: receiving an authenticated message, including a first authentication word and an appliance message, at the first appliance; generating a second authentication word by applying the first shared message counter, as stored in the first appliance, and the appliance message to an authentication algorithm; and comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message; a second appliance separate from the first appliance; and an appliance communication center including a second shared message counter and a third shared message counter, the second shared message counter shared between the appliance communication

center and the first appliance, the third shared message counter shared between the communication center and the second appliance, and the third shared message counter configured to provide a count separate from a count provided by the second shared message counter."

Neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest a system as recited in Claim 28. Specifically, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest an appliance communication center including a second shared message counter and a third shared message counter, the second shared message counter shared between the appliance communication center and the first appliance, the third shared message counter shared between the communication center and the second appliance, and the third shared message counter configured to provide a count separate from a count provided by the second shared message counter. Rather, Sharrow describes checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe incrementing a counter incremented by a sender and a receiver. Elgamal et al. further describe employing a pair of counters by the sender and the receiver for each transmission direction. Accordingly, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest an appliance communication center including a third shared message counter shared between the communication center and the second appliance separate from the first appliance, and the third shared message counter provides a count separate from a count provided by the second shared message counter. For the reasons set forth above, Claim 28 is submitted to be patentable over Sharrow in view of Elgamal et al.

Claim 29 depends from independent Claim 28. When the recitations of Claim 29 are considered in combination with the recitations of Claim 28, Applicants submit that dependent Claim 29 likewise is patentable over Sharrow in view of Elgamal et al.

Claim 30 recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at a first appliance a first non-

resettable shared message counter, the first non-resettable shared message counter shared between the first appliance and a remotely located appliance communication center; maintaining at the appliance communication center a second non-resettable shared message counter that counts messages communicated between the appliance communication center and the first appliance; maintaining at the appliance communication center a third non-resettable shared message counter that counts messages communicated between the appliance communication center and a second appliance, the third non-resettable shared message counter provides a count separate from a count provided by the second non-resettable shared message counter; generating a first authentication word by applying an appliance message and the first non-resettable shared message counter, as stored in the first appliance, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center."

Neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 30. Specifically, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest maintaining at the appliance communication center a second non-resettable shared message counter that counts messages communicated between the appliance communication center and the first appliance, and maintaining at the appliance communication center a third non-resettable shared message counter that counts messages communicated between the appliance communication center and a second appliance, the third non-resettable shared message counter provides a count separate from a count provided by the second non-resettable shared message counter. Rather, Sharrow describes checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe incrementing a counter incremented by a sender and a receiver. Elgamal et al. further describe employing a pair of counters by the sender and the receiver for each transmission direction. Accordingly, neither Sharrow nor Elgamal et al., considered alone or in combination, describe or suggest maintaining at the appliance communication center a second non-resettable shared message counter that counts messages

communicated between the appliance communication center and the first appliance, and a third non-resettable shared message counter that counts messages communicated between the center and a second appliance, where the third non-resettable shared message counter provides a count separate from a count provided by the second non-resettable shared message counter. For the reasons set forth above, Claim 30 is submitted to be patentable over Sharrow in view of Elgamal et al.

Claim 31 depends from independent Claim 30. When the recitations of Claim 31 are considered in combination with the recitations of Claim 30, Applicants submit that dependent Claim 31 likewise is patentable over Sharrow in view of Elgamal et al.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claims 16-19 and 23-31 under 35 U.S.C. 103(a) be withdrawn.

The rejection of Claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow in view of Elgamal et al., and further in view of Kaufman et al. (*Network Security: Private Communication in a Public World*), is respectfully traversed.

Sharrow and Elgamal et al. are described above.

Kaufman et al. describe a system in which sequence numbers have to be very large (page 242, fourth paragraph). Otherwise, there is a possibility of running out of the sequence numbers during a conversation (page 242, fourth paragraph). If the sequence numbers are reused during the conversation, an attacker can replay an old recorded message when a sequence number recurs (page 242, fourth paragraph).

Claim 20 depends indirectly from Claim 16 which recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication

center and the first appliance; maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter; generating a first authentication word by applying an appliance message and the first shared message counter, as stored in the communication center, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the first appliance."

None of Sharrow, Elgamal et al., and Kaufman et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 16. Specifically, none of Sharrow, Elgamal et al., and Kaufman et al., considered alone or in combination, describe or suggest maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter. Rather, Sharrow describes checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe incrementing a counter incremented by a sender and a receiver. Elgamal et al. further describe employing a pair of counters by the sender and the receiver for each transmission direction. Kaufman et al. describe having very large sequence numbers during a conversation. Otherwise, there is a possibility of running out of the sequence numbers during the conversation. Accordingly, none of Sharrow, Elgamal et al., and Kaufman et al., considered alone or in combination, describe or suggest maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and an appliance and that provides a count separate from a count provided by the first shared message counter. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Elgamal et al., and further in view of Kaufman et al.

When the recitations of Claim 20 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claim 20 likewise is patentable over Sharrow in view of Elgamal et al., and further in view of Kaufman et al.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claim 20 under 35 U.S.C. 103(a) be withdrawn

Moreover, Applicants respectfully submit that the 35 U.S.C. § 103 rejections of Claims 16-20 and 23-31 are not proper rejections. As is well established, obviousness cannot be established by combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. None of Sharrow, Elgamal et al., or Kaufman et al., considered alone or in combination, describe or suggest the claimed combination. Furthermore, in contrast to the assertion within the Office Action, Applicants respectfully submit that it would not be obvious to one skilled in the art to combine Sharrow with Elgamal et al. or Kaufman et al. because there is no motivation to combine the references suggested in the art.

As the Federal Circuit has recognized, obviousness is not established merely by combining references having different individual elements of pending claims. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP §2143.01. Rather, there must be some suggestion, outside of Applicants' disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicants' disclosure. In re Vaeck, 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case, neither a suggestion or motivation to combine the prior art disclosures, nor any reasonable expectation of success has been shown.

Furthermore, it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the cited art so that the claimed invention is rendered obvious. Specifically, one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the art to deprecate the claimed invention. Further, it is

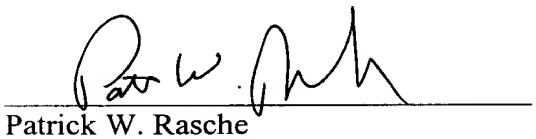
impermissible to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. The present 35 U.S.C. § 103 rejections are based on a combination of teachings selected from multiple patents in an attempt to arrive at the claimed invention. Specifically, Sharrow teaches checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. teach incrementing a counter incremented by a sender and a receiver. Elgamal et al. further teach employing a pair of counters by the sender and the receiver for each transmission direction. Kaufman et al. teach having very large sequence numbers during a conversation. Otherwise, there is a possibility of running out of the sequence numbers during the conversation. Because there is no teaching nor suggestion in the cited art for the combination, the 35 U.S.C. § 103 rejections appear to be based on a hindsight reconstruction in which isolated disclosures have been picked and chosen in an attempt to reject the claims of the present application. Of course, such a combination is impermissible, and for this reason Applicants request that the 35 U.S.C. § 103 rejections of Claims 16-20 and 23-31 be withdrawn.

For at least the reasons set forth above, Applicants respectfully request that the 35 U.S.C. § 103 rejections of Claims 16-20 and 23-31 be withdrawn.

Claims 21 and 22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants thank the Examiner for the indication of allowable subject matter.

In view of the foregoing remarks, this application is believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,



Patrick W. Rasche
Registration No. 37,916
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070